PCT/CN2004/001320

证　　明

本证明之附件是向本局提交的下列专利申请副本

申　请　日：　2003.11.21

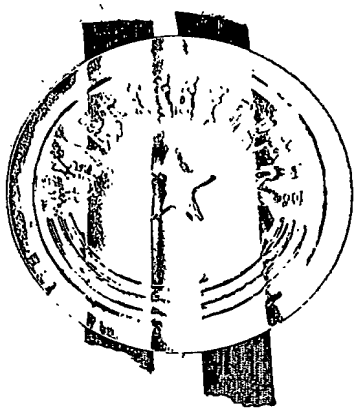
申　请　号：　200310115102X

申请类别：　发明

发明创造名称：　移动存储装置的数据管理方法

申　请　人：　深圳市朗科科技有限公司

发明人或设计人：　邓国顺



中华人民共和国
国家知识产权局局长　王景川

2004 年 12 月 8 日

权 利 要 求 书

1. 一种在具有可更换存储芯片的移动存储装置中的数据管理方法，其特征在于，该方法包括：

1) 确定所述存储芯片的使用情况，采用或组织或建立或重建所述移动存储装置存储介质的文件管理系统；和

2) 根据与所述移动存储装置连接的主机系统的操作指令，利用所述文件管理系统在所述存储芯片中进行相应的操作。

2. 根据权利要求 1 所述的数据管理方法，其特征在于，所述步骤 1）包括：

所述移动存储装置的控制器读取装入移动存储装置的存储芯片数量，以及获取所述每个存储芯片的存储容量信息。

3. 根据权利要求 2 所述的数据管理方法，其特征在于，进一步包括：

所述主机系统根据所述移动存储装置的存储芯片信息，产生一个或多个所述移动存储装置的盘符。

4. 根据权利要求 3 所述的数据管理方法，其特征在于：

所述移动存储装置盘符的个数与装入移动存储装置的存储芯片个数相一致。

5. 根据权利要求 3 所述的数据管理方法，其特征在于：

将所述移动存储装置的存储芯片划分成多个分区，所述移动存储装置盘符的个数与所述分区个数相一致。

6. 根据权利要求 1 所述的数据管理方法，其特征在于：

所述存储芯片包括已使用的存储芯片和/或未使用的存储芯片，所述未使用的存储芯片是指未经初始化或分区的原始芯片，并且，所述步骤 1）进一步包括：

确定所述存储芯片为已使用的存储芯片还是未使用的存储芯片，或

是包括已使用和未使用的存储芯片；

对于所述未使用的存储芯片，对该芯片进行格式化，建立文件管理系统；

对于仅有所述已使用的存储芯片的情况，采用其原有的文件管理系统，或重新组合、修改其文件管理信息，建立新的文件管理系统。

7. 根据权利要求 2 所述的数据管理方法，其特征在于：
所述装入的存储芯片是在现有移动存储装置的基础上装入的。

8. 根据权利要求 6 所述的数据管理方法，其特征在于：

所述已使用存储芯片的判断方法包括：读取所述存储芯片的逻辑“0”块，如果所述逻辑“0”块不全为逻辑“1”值，则说明所述存储芯片为已使用的；如果所述逻辑“0”块全为逻辑“1”值，则说明所述存储芯片为未使用的。

9. 根据权利要求 1 所述的数据管理方法，其特征在于：

所述文件管理系统类型包括支持 Windows 的文件管理系统及其升级版本，或者支持 UNIX 或 LINIX 的文件管理系统及其升级版本，

其中所述支持 Windows 的文件管理系统及其升级版本包括但不限于：FAT12、VFAT、FAT16、FAT32、CDFS、NTFS；

所述支持 UNIX 或 LINIX 的文件管理系统及其升级版本包括但不限于 EXT2、EXT3、JFFS、NFS、RAMFS、HPFS、CRAMFS。

10. 根据权利要求 1 所述的数据管理方法，其特征在于，所述在存储芯片中进行相应的操作包括步骤：

2-1） 读取所述操作指令中的指定地址，并将该指定地址转换为物理地址；

2-2） 将所述物理地址与所述存储芯片的容量进行比较，确定其所对应的存储芯片，并在所确定的存储芯片中找到对应的存储块。

11. 根据权利要求 10 所述的数据管理方法，其特征在于，进一步还包括：

2-3） 如果所述物理地址超出所述存储装置的全部存储芯片的存储容量，则所述移动存储装置返回错误信息。

12.根据权利要求 1 所述的数据管理方法，其特征在于，进一步还包括：

当对所述移动存储装置更换存储芯片时，所述主机系统停止对所述移动存储装置或该移动存储装置的控制器供电。

13.根据权利要求 1-8 任一项所述的数据管理方法，其特征在于：

在所述存储芯片中设置数据加密区，通过所述移动存储装置的控制器对存储的数据进行加密或解密处理。

说 明 书

移动存储装置的数据管理方法

技术领域

本发明涉及数据存储领域，具体地说涉及对具有多个存储芯片并可进行存储芯片的增加、减少和更换的移动存储装置进行数据管理的方法。

背景技术

目前，采用存储介质进行数据存储的移动存储装置获得了广泛的使用，已取代软盘成为通用的便携式数据存储设备。但是，由于技术的限制，现有的移动存储装置大多数仅设置容量有限的存储介质，该存储介质大多封装在芯片中，焊接在移动存储装置的电路板上，不可拆卸。用户如果需要对超出存储设备容量的大量数据进行存储和转移时，就必须更换甚至购买新的移动存储装置。另外，如果移动存储装置中部分部件损坏，则可能不得不废弃整个移动存储装置，包括未损坏的控制器、存储芯片等，并且在存储芯片仍然完好的情况下丢失用户的数据。上述两方面的缺陷限制了移动存储装置的应用范围，造成使用不便和浪费，也不利于用户数据的安全保障。

中国专利申请“存储介质固定装置及使用该固定装置的移动存储器”（申请号：03159669.X）公开了一种可更换存储芯片的移动存储装置，该存储装置可更换或扩充移动存储装置的存储芯片，使得移动存储装置能够随时改变存储容量，方便数据存储。但该专利申请公开的只是一种存储芯片的固定装置和使用该固定装置的移动存储装置，这种移动存储装置在更换芯片时可能不能正常使用或者可能会造成芯片中现有数据的丢失，不利于用户数据安全，从而限制了该移动存储装置的应用范围。

发明内容

本发明鉴于现有技术的不足和数据安全存储的目的，提出一种移动存储装置的数据管理方法，可以使更换芯片后的移动存储装置能够正常工作，并且可以提高用户数据的安全性。

为实现本发明的上述目的，提供一种在具有可更换存储芯片的移动存储

装置中的数据管理方法，该方法包括：根据所述存储芯片的使用情况，采用或组织或建立或重建所述移动存储装置存储介质的文件管理系统；根据与所述移动存储装置连接的主机系统的操作指令，利用所述文件管理系统在所述存储芯片中进行相应的操作。

所述主机系统可根据所述移动存储装置的存储芯片信息，产生一个或多个所述移动存储装置的盘符。

所述确定存储芯片的使用情况是指所述移动存储装置的控制器读取装入移动存储装置的存储芯片数量，以及获取所述每个存储芯片的存储容量信息。

所述移动存储装置包括：主机接口，用于移动存储装置与主机系统的连接；控制器，用于控制移动存储装置的操作；存储芯片固定装置，其中以可拆卸的方式固定安装有至少一个存储芯片，所述存储芯片通过所述存储芯片固定装置与所述主机接口和控制器电连接，在所述控制器的控制下进行数据读写。

本发明所述的存储芯片是指半导体存储芯片，包括闪存（Flash Memory）、DRAM、EEPROM、SRAM、SDRAM、FRAM 或 MRAM 等等；所述存储芯片可以是已使用的存储芯片，即所述存储芯片是经过系统初始化或进行过分区的或进行过数据存取的；同时也可以是未使用的存储芯片，即所述存储芯片是指芯片生产厂家出厂时的原始芯片，且没有经过任何使用的存储芯片。

所述文件管理系统类型包括但不限于 Microsoft 公司支持的 FAT12、VFAT、FAT16、FAT32、CDFS、NTFS 或其他可用于 Windows 的文件管理系统及其升级版本；或者 EXT2、EXT3、JFFS、NFS、RAMFS、HPFS、CRAMFS 或其他可用于 UNIX 或 LINIX 的文件管理系统及其升级版本。

采用本发明提供的移动存储装置数据管理方法，可以实现移动存储装置容量扩充、存储介质更换或者更新，以及使用所述可拆卸的存储芯片进行数据存储，提高了移动存储装置的应用功能和利用率，为用户使用提供方便，提高了数据安全性及系统易用性。

附图的简要说明

图 1 示意性地说明本发明使用的可拆卸更换存储介质的移动存储装置结构；

图 2 是本发明第一个实施方案实现移动存储装置与主机连接及数据操作的流程图；

图 3 是本发明移动存储装置的数据操作具体实施方法的流程示意图；

图 4 是在本发明中的存储芯片加密策略对照表示意图；

图 5 是对存储芯片的加密数据区进行数据操作地流程示意图；

图 6 是本发明实现移动存储装置与主机保持接口连接情况下拆卸存储介质的方法流程图。

具体实施方式

通过以下参照附图对本发明具体实施方案的详细说明，本领域技术人员将更易于理解本发明的思想和实质。

如图 1 所示，本发明可适用于可拆卸更换存储介质的移动存储装置，该移动存储装置除包括主机接口 1、控制器（未图示）和封装在存储芯片 2 中的存储介质外，还包括一固定装置。存储芯片可拆卸地固定安装在该固定装置内。所述固定装置包括底座 3 和上盖 4，所述底座 2 设置有弹性电连接部件 31。该弹性电连接部件 31 与放置于底座 3 内的存储芯片 2 以及底座 3 外的主机连接器 1 和控制器电连接。该弹性电连接部件 31 以可拆卸方式压紧存储芯片 2。

本发明使用的移动存储装置中的固定装置可以容纳两片或更多片的存储芯片 2。该固定装置的底座 3 上设置的连接部件 31 可以与每一个存储芯片 2 的管脚电连接，该连接部件 31 还设置有与每一个存储芯片 2 对应的片选引脚。该片选引脚分别单独与每一个存储芯片对应的片选管脚相连接，其他引脚则与存储芯片 2 的其他管脚对应连接。

以下将说明将存储芯片 2 装入移动存储装置后，移动存储装置对芯片 2 的初始化过程。

根据现有的操作系统技术规范，文件管理系统(以下以常用 FAT 表为例)是对存储空间进行管理的重要工具，操作系统对存储空间中的数据文件进行操作必须依据该 FAT 表。该表记录着每个簇的使用分配情况及磁盘数据的

存储地址,每一个文件都有一组连接的FAT链指定其存放的簇地址。FAT表的损坏将导致文件和数据内容的丢失。

根据现有的半导体存储技术和规范，未经使用的存储芯片的存储空间中所有位都是逻辑"1"，不包含任何数据信息；而已使用的存储芯片中存在数据及FAT表，其存储空间中不都是逻辑"1"，逻辑"0"块中必然不都是逻辑"1"。根据这一区别，通过读取存储芯片的逻辑"0"块的信息即可判断该存储芯片是否是未经使用的。

在本发明的移动存储装置中，用户可将多个存储芯片一次性装入移动存储装置，也可在原有的存储芯片上再叠加芯片。或者还可以是在现有移动存储装置的基础上再设置如本发明所应用的存储芯片固定装置，通过该存储芯片固定装置进行存储芯片的增加和/或更换。所谓现有移动存储装置是指该移动存储装置的部分存储芯片是固定不可拆卸的。

对于用户装入的存储芯片，移动存储装置要检测其是否为使用过的芯片，即未被初始化或分区的芯片。如果该芯片是从未使用过的空白芯片，移动存储装置将对其进行格式化，写入FAT表。如果该芯片是已使用的，已存在FAT表，就不需对芯片进行格式化，可以直接使用；

对于用户将包括已使用的芯片在内的两个及两个以上的芯片共同装入移动存储装置的情况，移动存储装置需对所有芯片进行排序和整理，再统一进行初始化处理，组合已使用的芯片中的FAT表信息，产生一个用于管理所有存储芯片的存储空间的FAT表。该FAT表对所有装入移动存储装置的存储芯片进行统一的组织管理，以供正常使用。

为保护已使用的芯片内的有用数据，对多个芯片中已使用的那些芯片，须将其中的FAT表进行组合、修正或重新编排，使FAT表能够管理整个存储装置内部的数据，并保证数据文件的安全。

具体的初始化过程如下：

用户将N个已使用的芯片和M个未使用的芯片装入移动存储装置中，再将该移动存储装置接入主机。在通过主机接口供电后，移动存储装置的控制器自动读取所有装入移动存储装置的存储芯片的序号（ID），确定存储芯片的数量，并取得所有存储芯片的容量。

然后，控制器对芯片进行排序。具体过程是，控制器按照芯片序号顺序

或片选顺序，依次读取每个芯片的逻辑“0”块，直到读到第一个逻辑“0”块不为全逻辑“1”值的芯片（即已使用的芯片），将其作为物理地址第 0 芯片。接下来用同样的方式，找出所有逻辑“0”块不为全逻辑“1”值的 N 个芯片，将它们依次作为物理地址第 1 芯片、物理地址第 2 芯片.....物理地址第 N 芯片。所述逻辑 “0” 块是对存储芯片编逻辑地址时的起始块，即逻辑地址的第一块。根据现有操作系统和磁盘管理规范，FAT 表及对照表应写入该块中。

接着，控制器再将剩余的逻辑“0”块为全逻辑“1”值的 M 个芯片（即未使用芯片）依次编为物理地址第 N+1 芯片、物理地址第 N+2 芯片...物理地址第 N+M 芯片。

至此，芯片排序完毕。按照该顺序排序的多个芯片，其物理地址从物理地址第 0 芯片开始，顺序连续至物理地址第 N+M 芯片结束。移动存储装置的总存储空间为所有芯片的存储空间之和。

接下来，控制器将前述 N 个已使用过的芯片中的文件信息进行整理，重新组织并变换地址。地址的变换是依据上述存储芯片排序的方法，数据文件信息的管理原则是依据 FAT 文件系统管理的方法，再根据实际存储地址发生变更的结果（即已经使用过的 N 个芯片的物理存储区的相对地址已经因排序产生变化）重新产生主机系统能够识别的 FAT 文件系统，将总存储空间和所有数据文件的新地址信息整合为新的 FAT 表，根据控制器默认地址写入存储芯片中（默认地址是由存储芯片排序结果确定，整合方法与原理是 FAT 文件系统的管理方法）。

如果 N 为 0，即用户装入移动存储装置的全部是未使用过的芯片，则移动存储装置的控制器在排序完毕后，毋须进行文件地址的变换，直接将存储空间组织写入 FAT 表。

在每次用户改变移动存储装置的存储芯片，例如增加、替换、移除芯片后，控制器都应对所有装入移动存储装置的存储芯片进行上述初始化过程。

以下，将以移动存储装置安装两个存储芯片的情况为例介绍根据本发明由移动存储装置的控制器对存储芯片进行操作的过程。

在本实施方案中，移动存储装置安装有两个存储芯片，第一芯片采用 64M 容量的快闪存储芯片，第二芯片采用 128M 容量的快闪存储芯片。第一芯片、第二芯片依次固定安装在所述固定装置内。本实施方案的主机连接器

采用符合 USB 标准的通用接口，通过标准 USB 接口与主机进行连接和数据交换。

根据计算机的数据存储结构以及相关标准，存储空间划分为多个存储块，每个存储块划分为多个页，页中包含有存放地址信息的区域，存储块的逻辑地址与对照表中的地址信息具有对应关系。根据数据操作指令中的指定地址，通过地址变换可得出相应的指定逻辑地址（以下统称为指定逻辑地址）。根据该指定逻辑地址查找对照表，找出与指定逻辑地址相应的逻辑地址，再找出与该逻辑地址对应的物理地址，就可以从存储介质中找到指定的存储块。上述对指定地址的地址变换操作可以采用现有的地址变换技术进行。

在本实施方案中，移动存储装置的存储空间由存储容量不同的第一芯片和第二芯片组成。通过上述的初始化过程后，第一芯片作为存储空间中的物理地址第 0 芯片，第二芯片作为存储空间中的物理地址第 1 芯片，这两个芯片内存储空间的物理地址是连续的。第一芯片的物理地址以 0 作为起始地址，以 63 作为结尾地址；而第二芯片以 64 作为起始地址，以 191 作为结尾地址。

本实施方案的移动存储装置可根据主机发来的操作指令，按照各个存储芯片的容量进行芯片的选择和寻址。指令寻址及芯片选择过程如下：

读取数据操作指令中的指定地址，将该指定地址经上述地址变换过程变换为物理地址，将得到的物理地址与第一芯片的容量进行比较。

如果该物理地址不超出第一芯片的容量，说明该指定的物理地址位于第一芯片中，此时在第一芯片中找到对应存储块即可；如果物理地址超出第一芯片的容量，说明该指定的物理地址可能位于第二芯片中。此时应将得到的物理地址与第一芯片、第二芯片的容量之和进行比较，如果物理地址超出第一芯片、第二芯片的容量和，说明该指定的物理地址超出存储空间范围，所述控制器返回错误信息。如果物理地址不超出第一芯片、第二芯片的容量之和，说明该指定的物理地址位于第二芯片中，此时在第二芯片中按指定的物理地址找到对应存储块即可。

如果移动存储装置中固定安装有N个芯片，则寻址方式与上述步骤类似，将指定物理地址逐次与芯片从一到 N 的容量累加值比较，直到找出包含指定物理地址的芯片；如果所有芯片的容量和小于指定物理地址，说明指定物理地址超出范围，控制器返回错误信息。

本实施方案的移动存储装置可具有身份认证机制，该身份认证机制可实现对主机的访问控制和对移动存储装置的访问控制。上述两种访问控制都需用户通过身份认证。用户可对身份认证机制进行设置，设置项目包括启用/禁用身份认证机制、用户名及密码、访问权限、身份认证机制设置权限等。移动存储装置根据用户设置的身份认证机制进行访问控制。

本实施方案的移动存储装置还支持多用户的使用。多个用户之间通过用户名区分，每个用户可拥有虚拟存储空间。该虚拟存储空间可对其他用户隐藏或开放，虚拟存储空间大小可变。所述多用户策略可采用现有技术实现。例如，可通过加密闪存盘技术，概括地说，就是控制器依据不同用户的需求，通过将存储芯片连续容量折分成多个具有一定容量的存储块，从而为每个用户分配一个特定容量的存储盘。对这些不同的用户，其能操作的空间是被分配的虚拟空间和共用的存储空间，并且具有特定的访问密码。

图 2 示出了上述实施方案的移动存储装置与主机连接及数据操作的流程：

如图 2 所示，在步骤 1，用户将第一芯片和第二芯片依次安装在移动存储装置的固定装置上，使存储介质与移动存储装置的主机连接器、控制器等部件建立电连接。然后，将移动存储装置通过主机连接器接入到主机的对应接口（步骤 2）。主机的对应接口检测到有设备接入，将向接入的移动存储装置供电（步骤 3）。

接着，主机向移动存储装置发出问询指令，询问移动移动存储装置的描述符。移动存储装置根据问询指令，从控制器中获取设备描述符。该设备描述符含有标志，表明移动存储装置允许产生多个盘符。移动存储装置将该设备描述符返回给主机（步骤 4）。主机接收到该描述符后，为移动存储装置分配逻辑地址（步骤 5）。

接下来，主机再次发出问询指令，询问配置、端点、接口描述符，移动存储装置根据该问询指令获得上述描述符返回给主机（步骤 6）。所述描述符包含支持最大逻辑单元（LUN）数的信息，即要求产生多少个盘符的标志。主机对返回的描述符进行检验，检查描述符是否符合规范（步骤 7），如果不合规范则禁止配置该设备，返回到第一次问询描述符之前，再次进行询问（步骤 8'）。如果第三次获得的描述符仍不符合规范，则停止询问，不再进

行设备的配置。

如果描述符符合规范，则主机向移动存储装置发出准许配置设备的指令（步骤 8），开始进行一系列移动存储装置配置操作：

主机发出问询指令，询问设备相关信息（步骤 9），该信息包括设备厂商名、产品名、存储容量等，启动相应设备驱动程序，选择接口、端点（管道），确定传输方式。移动存储装置应答该问询指令，返回上述信息（步骤 10）。主机根据移动存储装置的要求，为移动存储装置分配一个或多个盘符（步骤 11）。至此，主机对移动存储装置的识别、配置过程完毕。本发明所述移动存储装置盘符的个数可以与装入移动存储装置的存储芯片个数相一致；也可以将所述存储芯片划分成多个不同的分区，从而产生移动存储装置盘符的个数与所述分区个数相一致。

接下来，主机接收用户对移动存储装置的操作指令，将指令转发给移动存储装置（步骤 12）。移动存储装置的控制器接收操作指令（步骤 13）后，解释、执行指令（步骤 14），将指令执行结果、系统信息、操作数据等返回主机（步骤 15）。重复上述过程执行用户指令直到用户发出指令要求移除移动存储装置（步骤 16）。

在接收到用户发出的移除移动存储装置指令后，主机保存用户的信息（步骤 17），完成该用户的所有操作任务，停止对移动存储装置供电（步骤 18），此时移动存储装置与主机断开连接，整个流程结束。

在上述流程中，对移动存储装置的基本操作指令有读数据、写数据、格式化操作，还可以包括切换用户和身份认证等操作，对于不同类型的操作，移动存储装置的执行过程不同，图 3 示出了数据操作具体实施方法的流程，参考图 3 详述如下：

对于身份认证操作，主机要求用户输入认证信息，并将该用户输入的认证信息传送给移动存储装置。移动存储装置将该认证信息与其存储介质中预存的认证信息进行比较。如果认证信息与预存信息相符，则确定用户对移动存储装置的操作权限并向主机返回认证成功信息。如果认证信息与预存信息不符，则向主机返回认证失败信息。操作流程回到图 2 的①，移动存储装置继续等待主机下达下一操作指令。

例如，根据身份认证机制的设定，用户必须通过移动存储装置进行身份

认证才能对主机进行数据操作。在用户要对主机进行数据操作之前，主机弹出对话框要求用户输入用户名、密码等认证信息。该认证信息通过主机对应接口按照接口规范打包传送给移动存储装置的主机接口连接器，主机接口连接器接收到数据后传送给移动存储装置的控制器。控制器将该认证信息与预先设定或预先存储的认证信息进行核对。如果核对正确，则控制器根据身份认证机制确定该用户对主机具体的操作权限（例如只读、读写、格式化、身份认证机制的设置权限等），并进行标记，返回认证通过信息。如果核对不正确，则向主机返回认证失败信息。返回给主机的认证失败信息通过主机连接器传送给主机的对应接口，由主机反馈信息给用户。上述认证过程结束后，移动存储装置等待接收主机的下一操作指令。

对于根据身份认证机制，用户对移动存储装置进行操作必须通过身份认证的情况，其认证处理流程与上述流程类似，不再赘述。

对于读数据操作指令，例如用户需要将指定的存储芯片中的指定数据读取出来，移动存储装置的控制器先检验该用户的操作权限，确定该用户是否拥有对存储介质的读操作权限。如果用户不具备读数据权限，则向主机返回操作失败信息。操作流程回到图 2 的①，移动存储装置继续等待主机下达操作指令。如果用户具有读数据权限，则从指定的存储介质中读取指令指定的数据，根据用户设定，判断该笔数据是否经过加密和需要解密。如果需要解密，则移动存储装置的控制器调用加密策略对该笔数据进行解密后返回给主机；如果该笔数据不需解密，则直接返回给主机。

当然，如果移动存储装置内没有设置数据加密策略，则不需对读出的数据进行加密解密处理。

对于写数据操作指令，例如用户需要将指定数据写到移动存储装置的存储介质中，指令的处理类似于读数据操作指令：移动存储装置的控制器先检验该用户的操作权限，确定该用户是否拥有对该移动存储装置的存储介质的写操作权限。如果用户不具备写数据权限，则向主机返回操作失败信息。操作流程回到图 2 的①，移动存储装置继续等待主机下达操作指令。如果用户具有写数据权限，则根据身份认证机制的设定判断该笔数据是否需要加密。如果需要加密，则移动存储装置的控制器调用加密策略对该笔数据进行加密后写入存储介质，再向主机返回写数据成功信息。如果该笔数据不需加密，

则直接写入存储介质，并向主机返回写数据成功信息。

同样地，如果移动存储装置内没有设置数据加密策略，则不需对要写入的数据进行加密解密处理。

对于格式化操作指令，移动存储装置的控制器同样要先检验该用户的操作权限，确定该用户是否拥有对移动存储装置存储介质的格式化操作权限。如果用户不具备该操作权限，则向主机返回操作失败信息。操作流程回到图2的①，移动存储装置继续等待主机下达操作指令。如果用户具有该操作权限，则对存储介质进行格式化操作，并向主机返回格式化成功信息。

当移动存储装置的多个用户之间进行切换时，要进行切换用户操作。具体处理是：主机接收用户下达的退出指令并转发给移动存储装置，移动存储装置保存当前用户的信息，主机重置移动存储装置，操作流程回到图2的①，移动存储装置继续等待主机下达操作指令。只有下一位用户完成身份认证操作后，才可以访问移动存储装置。

在上述方法的基础上，还可以对移动存储装置进行改进和应用功能的扩展，例如可由用户指定对移动存储装置设置盘符的数目、具体的每个盘符以及盘符的图标。所述对盘符的数据、符号、与存储介质地对应关系及图标的设置可采用现有技术，通过软件程序实现。

本发明还可以由用户自行设置每个存储芯片或盘符中加密数据区，并可指定加密数据区的大小。用户可进一步对存储芯片或盘符的加密数据区单独设置加密策略。具体的方法将在下文中说明。对于设置了加密数据区的存储芯片，未经加密的数据仅能存放在非加密数据区中，而所有存入加密数据区的数据必须经过加密策略的加密处理，这些数据读出时也必须通过加密策略进行解密处理。

在对存储芯片或盘符对应存储空间进行数据操作时，移动存储装置的控制器将根据用户的加密数据区设置情况以及指令所指定的地址，确定数据操作是否需要通过加密解密处理。对于需要进行加密/解密处理的数据，移动存储装置将根据上述设置单独采取数据加密解密处理；对于不需进行加密解密处理的数据，按照常规数据操作方法进行操作。

对存储芯片设置加密数据区，修改加密数据区大小的具体实现方法是：控制器在存储芯片中根据主机系统的选择设置若干信息位，这些信息位用于

表明该存储芯片中是否设有加密数据区及其大小。控制器根据这些信息位可得知是否有加密数据区及其大小。加密数据区的起始地址由控制器根据预先设定给出。如果用户需要改变对加密数据区的设置，例如取消加密数据区、改变加密数据区的大小等，仅需发出指令，由控制器控制改写这些信息位的内容即可。

对存储芯片的加密数据区进行数据操作的具体做法如下：

图 4 所示为在移动存储装置中设置存储芯片加密策略的对照表。该对照表中包括序号、加密策略等项目，其中加密策略项目包括加密算法、密钥等信息，表中每个需要进行加密解密处理的存储芯片或每个盘符都对应一种加密策略和采用该种加密策略所需要的信息。用户可通过软件程序向移动存储装置装入加密策略，并在该对照表中指定该加密策略应用于那些存储芯片上。如果用户不对存储芯片的加密数据区指定加密策略，则移动存储装置将采用默认的加密策略，对该加密数据区进行加密解密处理。需要说明，此处仅仅针对加密区，非加密区是不经过加密的。

图 5 显示了对加密数据区进行数据操作的流程。同时参照图 2 和图 3 的操作流程，在移动存储装置接收到数据操作指令后，控制器分析数据操作指令属于读命令还是写命令，通过前述指令寻址过程确定指定地址位于哪一个存储芯片中，再根据该存储芯片的序号查找存储芯片加密策略对照表。如果在对照表中查找不到该存储芯片的序号，说明用户仅对该芯片设置了加密数据区，而没有指定加密策略。此时控制器采用默认的加密策略，使用预存在移动存储装置中的加密算法对数据进行读写过程中的加密解密处理。如果能够找到对应芯片序号的记录，说明用户为该芯片单独指定了加密策略，则控制器根据加密策略找出存储在移动存储装置中的加密算法，对数据进行读写过程中的加密解密处理。

在上述操作完成后，控制器将根据操作完成情况向主机返回系统信息。

对盘符设置加密数据区及其加密策略实际上是对一个或多个对应于该盘符的存储芯片设置加密数据区及其加密策略。故当用户对某个盘符设置加密数据区及其加密策略后，控制器只需根据盘符与存储芯片的对应关系，将对盘符的加密数据区和加密策略设置转换为对存储芯片单独的设置即可。在进行数据操作时，将对盘符的数据操作指令分解为对其对应的存储芯片的数

据操作指令，再采用上述在一个设有加密数据区的存储芯片内进行数据操作的具体做法，进行数据读写操作过程中的加密解密处理。

以上是对本发明的一个实施方案的描述。该实施方案可实现具有可拆卸更换存储介质的移动存储装置同主机的连接、识别、配置和数据操作，还能根据加密策略对各个存储芯片及盘符的数据分别进行加密解密处理，能够根据身份认证机制对访问主机和移动存储装置的用户进行身份认证和访问权限控制。

但该实施方案存在不足之处：如果用户需要在使用过程中更换、拆卸、增加存储芯片，按照现有技术必须发出指令将移动存储装置移除，待主机停止对移动存储装置供电后，将移动存储装置从主机接口上拔出或取下移动存储装置，安装存储芯片后再次插入主机接口，重新开始与主机的连接、识别、配置过程。复杂的操作不便于用户使用移动存储装置，如果主机尚未断电用户就非法拔出移动存储装置，还有可能造成移动存储装置的损坏。

针对上述问题，本发明提出了另一种实施方案，以实现移动存储装置与主机保持连接情况下拆卸存储芯片。此移动存储装置的主机连接器也采用符合 USB 标准的通用接口，通过标准 USB 接口与主机进行连接和数据交换，其流程图如图 6 所示。

参照图 2，在用户将移动存储装置接入主机对应接口后，主机对应接口检测有设备接入，通过接口向移动存储装置供电，连接、识别、配置移动存储装置，配置成功后主机对移动存储装置转发用户操作指令，进行数据操作。当用户发出指令要求对存储芯片进行拆装时，主机在接收到移除指令后，结束该用户所有任务，保存用户信息，然后停止向移动存储装置的控制器供电。上述过程与图 2 所示流程类似。

在主机停止向移动存储装置的控制器供电后，主机向用户返回信息，提示用户可以安全地对移动存储装置中的存储芯片进行拆卸/安装操作。用户毋须将从主机接口中拔出移动存储装置，就可以直接对其进行拆卸、更换存储芯片的操作。在拆卸、更换存储芯片后，用户再次发出指令，通知主机重新接入移动存储装置。主机接收到用户指令后，返回到图 6 的步骤 1 之后，通过对应接口再次向移动存储装置的控制器供电，再次执行连接、识别、配置过程。由此，本方法解决了反复插拔移动存储装置的不便问题，以及带电插

拔容易损坏移动存储装置的问题，还扩充了移动存储装置的应用功能，提高了数据安全性和装置易用性。

上述方案中，用户可以通过软件发出移除、重新安装移动存储装置的指令；也可以通过开关实现。该开关可设置在移动存储装置上，与移动存储装置的供电部件相连，在主机对移动存储装置的控制器断电后，主机与移动存储装置的接口间还保持供电待命状态。用户通过移动存储装置上的开关发出安装移动存储装置的信号。最简单的方法是，该开关直接控制移动存储装置所连接的主机 USB 接口提供的电源，安装存储芯片时，切断电源，安装完毕后接上电源。主机在下一次问询该接口上是否有设备接入时，回答为有设备接入，从而实现了通过手动开关来发出重新安装移动存储装置的指令。

以上是对本发明示例性的说明，本领域普通技术人员可以理解，本发明使用的移动存储装置以及移动存储装置中的固定装置，其具体实现方案不是唯一的；主机对移动存储装置进行识别配置的操作步骤也不是唯一的，是可利用现有技术进行调整的。为多个存储芯片分配物理地址、设置多个盘符，或按照用户要求对每个存储芯片或盘符进行加密策略的设置以及和身份认证机制的设置方法也可采用各种已知的技术。不偏离本发明思想的对本发明技术方案的各种改型将落入本发明权利要求所限定的范围中。

说 明 书 附 图

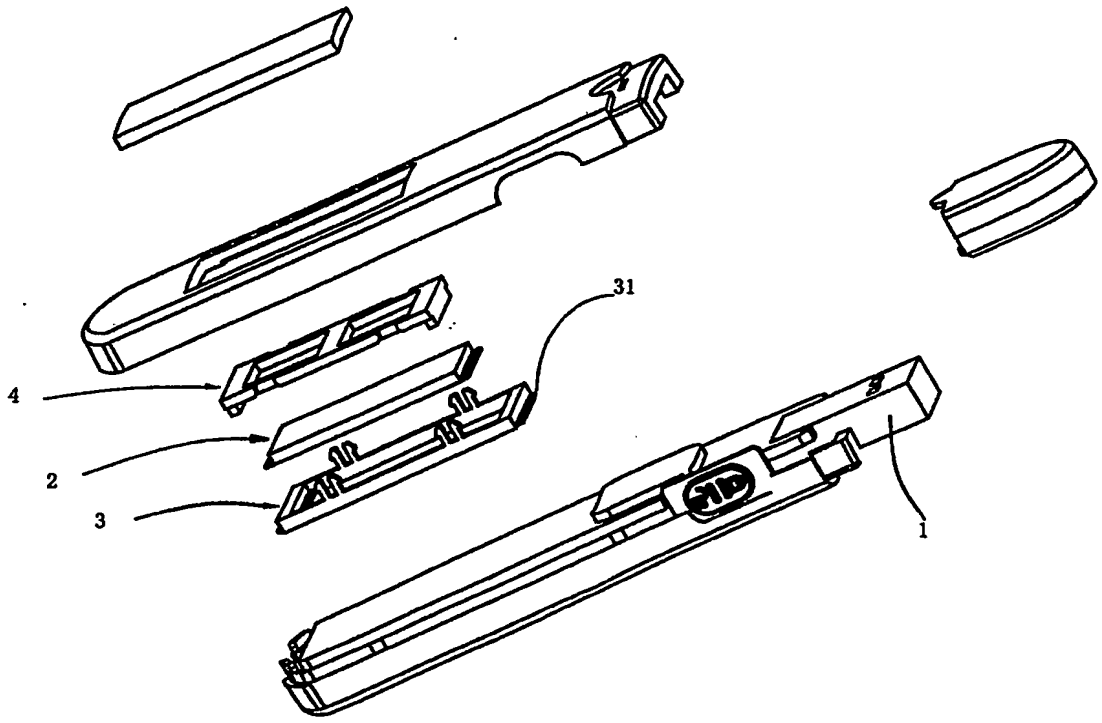


图 1

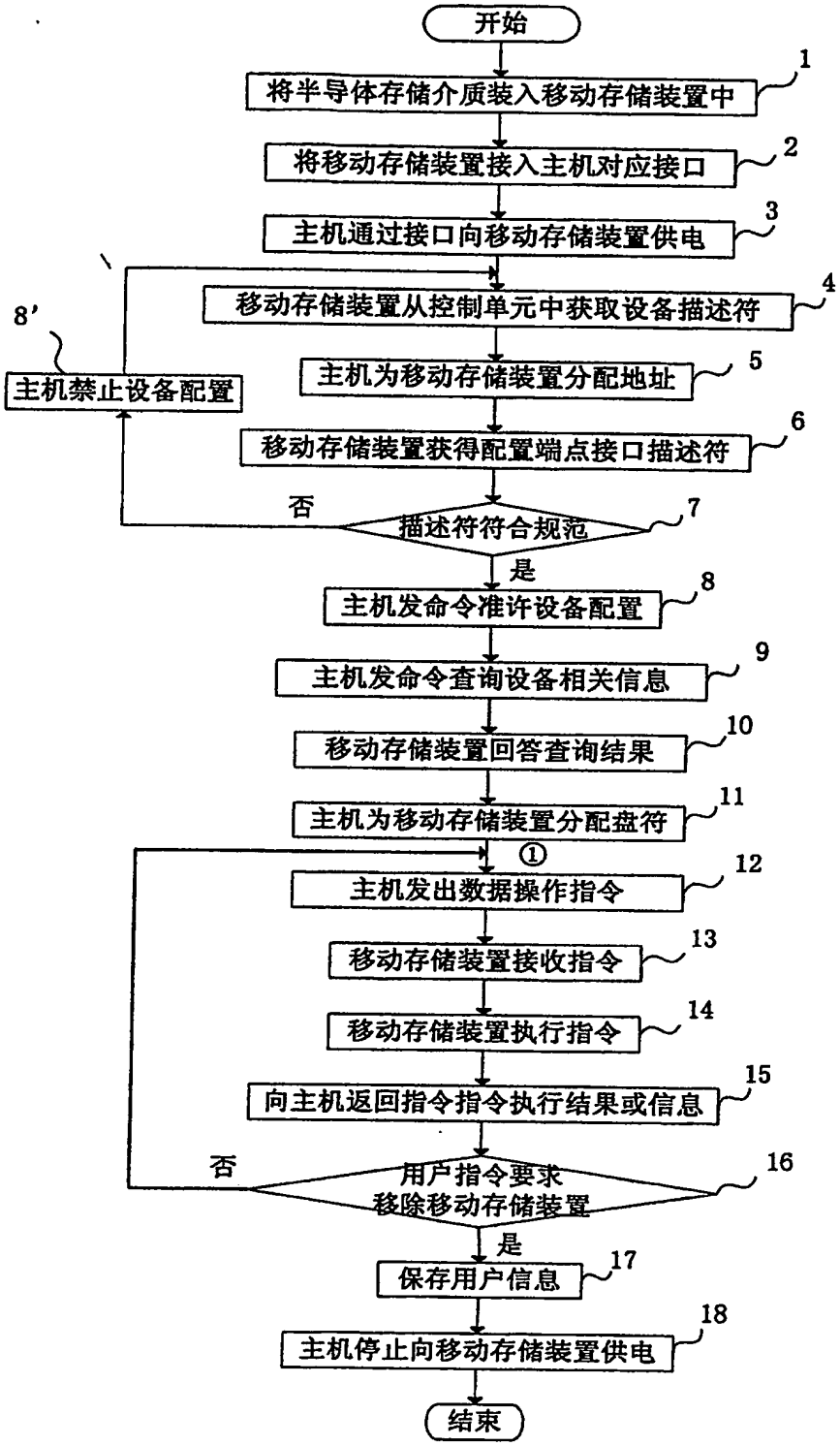

开始
将半导体存储介质装入移动存储装置中
1
将移动存储装置接入主机对应接口
2
主机通过接口向移动存储装置供电
3
移动存储装置从控制单元中获取设备描述符
4
主机为移动存储装置分配地址
5
移动存储装置获得配置端点接口描述符
6
描述符符合规范
7
否
是
主机禁止设备配置
8'
主机发命令准许设备配置
8
主机发命令查询设备相关信息
9
移动存储装置回答查询结果
10
主机为移动存储装置分配盘符
11
①
主机发出数据操作指令
12
移动存储装置接收指令
13
移动存储装置执行指令
14
向主机返回指令指令执行结果或信息
15
用户指令要求
移除移动存储装置
16
否
是
保存用户信息
17
主机停止向移动存储装置供电
18
结束

图 2

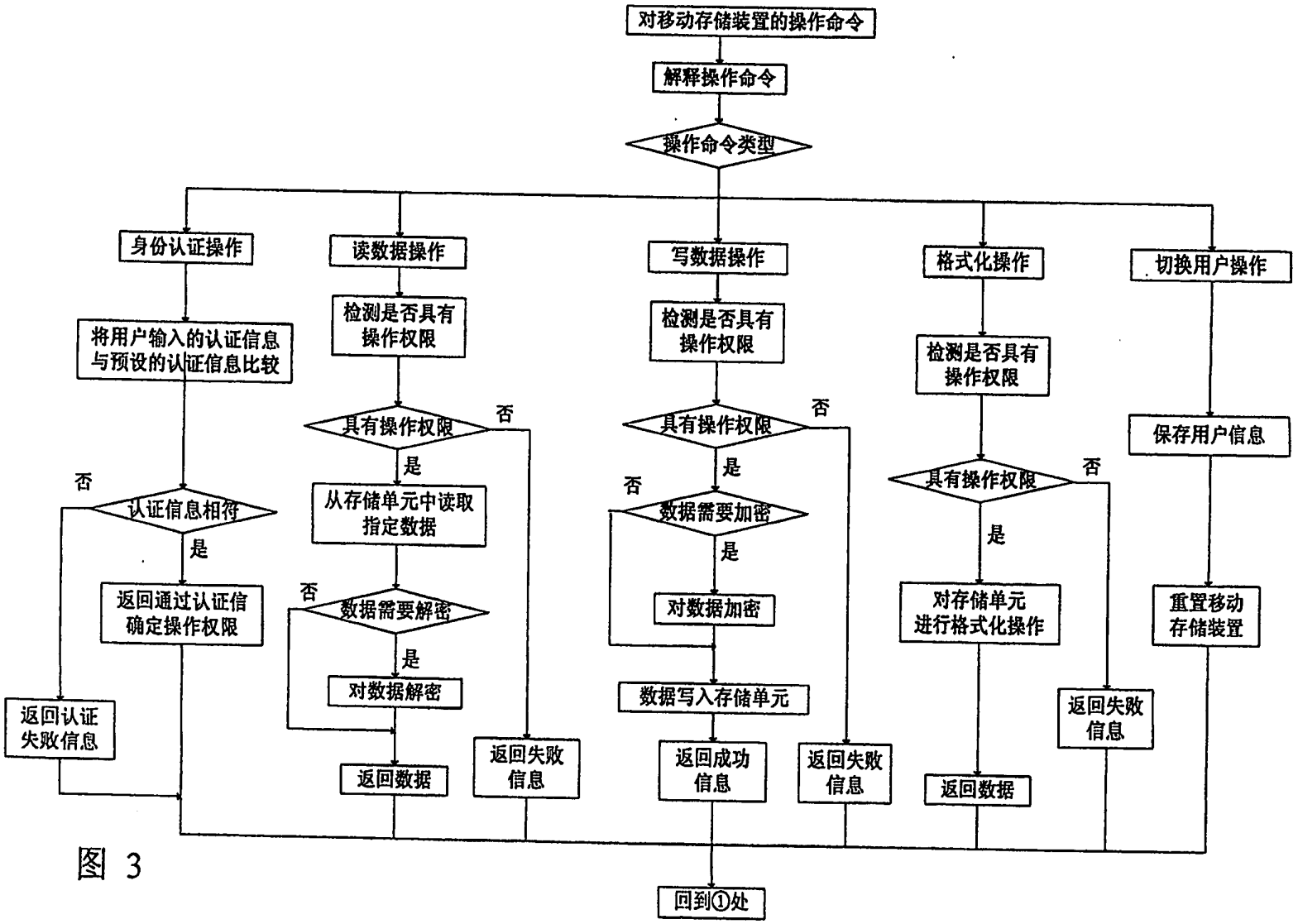

对移动存储装置的操作命令
解释操作命令
操作命令类型
身份认证操作
读数据操作
写数据操作
格式化操作
切换用户操作
将用户输入的认证信息与预设的认证信息比较
检测是否具有操作权限
检测是否具有操作权限
检测是否具有操作权限
保存用户信息
否
认证信息相符
具有操作权限
否
具有操作权限
否
具有操作权限
否
是
是
是
是
是
从存储单元中读取指定数据
数据需要加密
数据需要加密
对存储单元进行格式化操作
重置移动存储装置
返回通过认证信确定操作权限
否
数据需要解密
对数据加密
返回认证失败信息
是
对数据解密
数据写入存储单元
返回失败信息
返回数据
返回失败信息
返回成功信息
返回失败信息
返回数据
回到①处

图 3

芯片序号	加密算法	密钥	其他信息
1			
2			
⋮	⋮	⋮	⋮
N			

图 4

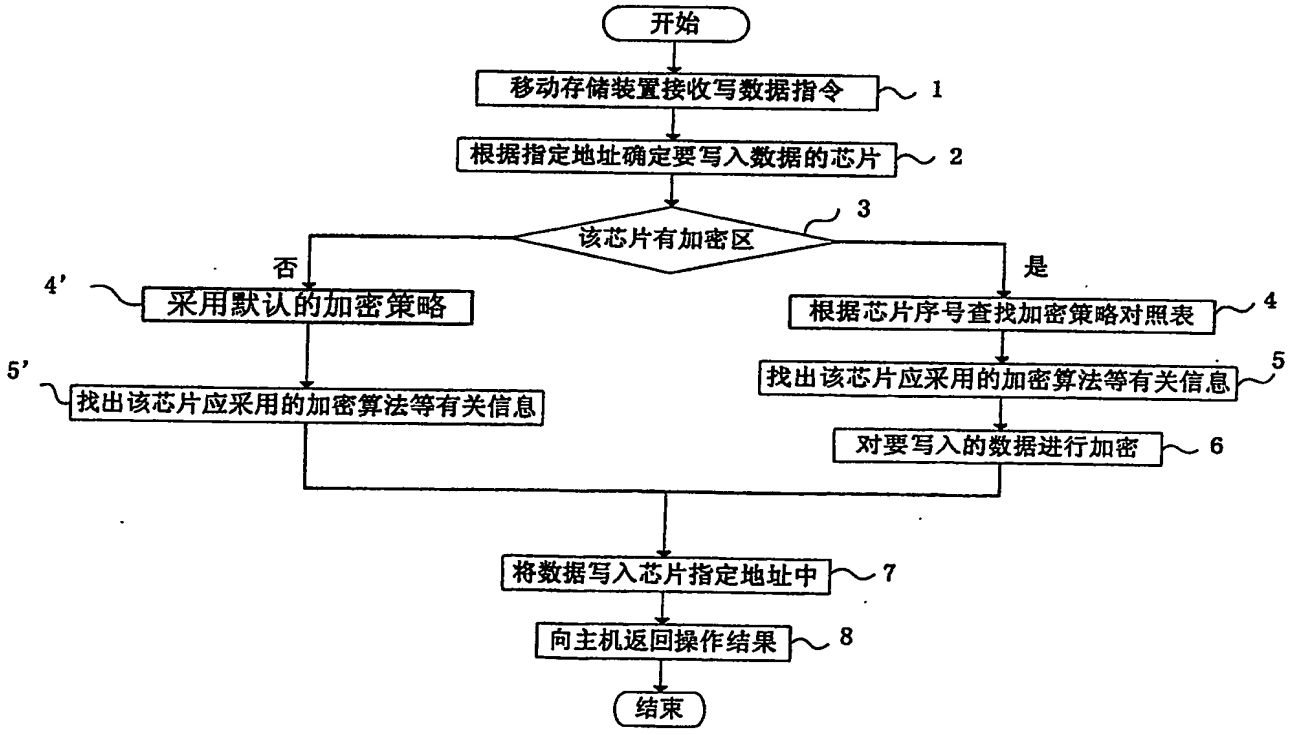


图 5

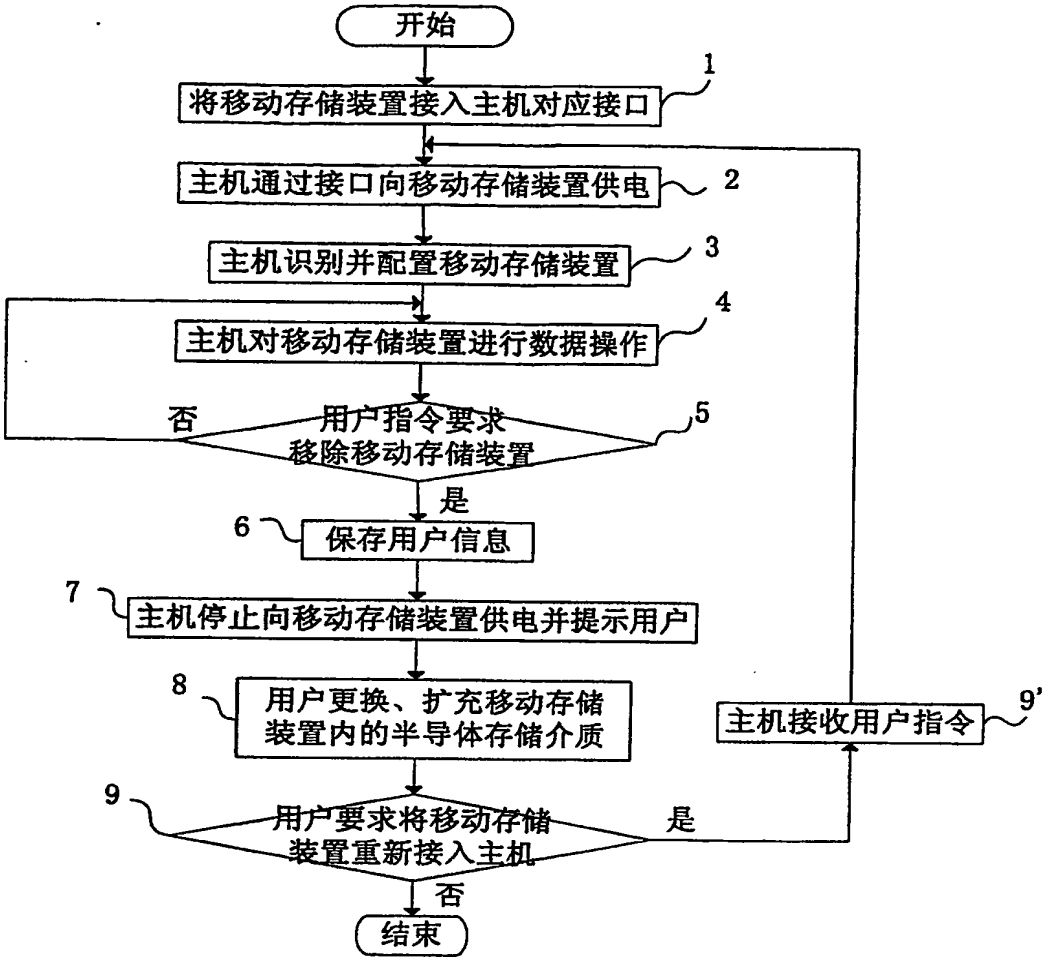

开始
1
将移动存储装置接入主机对应接口
主机通过接口向移动存储装置供电
2
主机识别并配置移动存储装置
3
4
主机对移动存储装置进行数据操作
否
用户指令要求
移除移动存储装置
5
是
6
保存用户信息
7
主机停止向移动存储装置供电并提示用户
8
用户更换、扩充移动存储
装置内的半导体存储介质
9
用户要求将移动存储
装置重新接入主机
是
否
结束
主机接收用户指令
9'

图 6

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/CN04/001320

International filing date: 19 November 2004 (19.11.2004)

Document type: Certified copy of priority document

Document details: Country/Office: CN
Number: 200310115102.X
Filing date: 21 November 2003 (21.11.2003)

Date of receipt at the International Bureau: 14 February 2005 (14.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)